BOISE MATTHEWS DONEGAN LLP
Bridget M. Donegan, OSB No. 103753
805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

Attorneys for Plaintiff Loujain Hathloul Alhathloul

FOLEY HOAG LLP
Christopher E. Hart, MA BBO No. 625031
chart@foleyhoag.com
Anthony D. Mirenda, MA BBO No. 550587
adm@foleyhoag.com
Andrew Loewenstein, MA BBO No. 648074
aloewenstein@foleyhoag.com
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1232

Attorneys for Plaintiff Loujain Hathloul Alhathloul

ELECTRONIC FRONTIER FOUNDATION
David Greene, CA Bar No. 160107
davidg@eff.org
Sophia Cope, CA Bar No. 233428
sophia@eff.org
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Attorneys for Plaintiff Loujain Hathloul Alhathloul

CENTER FOR JUSTICE AND ACCOUNTABILITY
Daniel McLaughlin, CA Bar No. 315326
dmclaughlin@cja.org
Claret Vargas, MA BBO No. 679565
cvargas@cja.org
Carmen Cheung Ka Man, NY Bar No. 4132882
ccheung@cja.org
268 Bush St. #3432
San Francisco, CA 94104
(415) 544-0444

Attorneys for Plaintiff Loujain Hathloul Alhathloul

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

LOUJAIN HATHLOUL ALHATHLOUL, *Plaintiff,* v. DARKMATTER GROUP, MARC BAIER, RYAN ADAMS, and DANIEL GERICKE *Defendants.*	Civil No. 3:21-cv-01787-IM **PLAINTIFF'S MOTION FOR LIMITED JURISDICTIONAL DISCOVERY AND TO HOLD IN ABEYANCE DEFENDANTS' JOINT MOTION TO DISMISS** **REQUEST FOR ORAL ARGUMENT**

LR 7-1 CERTIFICATION

Counsel for Plaintiff have conferred on this Motion with counsel for Defendants. The parties were unable to resolve the dispute forming the basis of this Motion.

MOTION

Plaintiff Loujain Alhathloul, by and through undersigned counsel, hereby moves for leave to conduct limited jurisdictional discovery as to Defendants DarkMatter, Marc Baier, Ryan Adams, and Daniel Gericke (collectively "Defendants") and to hold in abeyance Defendants' Joint Motion to Dismiss until the completion of jurisdictional discovery. Plaintiff Alhathloul further moves for an order that the parties confer and submit a joint proposed discovery and briefing schedule on jurisdictional discovery within 14 days of the Court's order.

INTRODUCTION

In order to resolve Defendants' Joint Motion to Dismiss for alleged lack of personal jurisdiction on a more satisfactory evidentiary record, Alhathloul requests limited discovery to

assess the nature and extent of Defendants' contacts with the forum. As set out in Alhathloul's Amended Complaint and Opposition to Defendants' Joint Motion to Dismiss, Defendants' actions to exfiltrate data from Alhathloul's iPhone while she was physically present in the United States establish a jurisdictionally adequate contact between Defendants, two of whom are U.S. citizens, and the forum. Defendants attribute their U.S. contacts solely to Alhathloul—and her choice to travel while her device was infected with malware—even though Defendants imposed their malware on Alhathloul without her knowledge or consent and continued using it to exfiltrate her data, including during her travel to the United States. Defendants' Reply attempts to minimize the jurisdictional significance of this conduct by mischaracterizing Alhathloul's allegations, arguing that Alhathloul somehow alleges "no such actions" to exfiltrate her data. Defendants also contend that Alhathloul has pled insufficient detail to support her argument that Defendants selected U.S.-based anonymization services and proxy servers *because of* their U.S. connection. Alhathloul should be granted limited discovery to gather facts—all of which would only be within the exclusive control of Defendants—to test the veracity of Defendants' characterizations and so that the dispute can be resolved on a more developed record.

ARGUMENT

Despite claiming to have "accepted the truth of all non-conclusory allegations for purposes of this Court's personal jurisdiction analysis," Defendants' Reply relies on mischaracterizations of Plaintiff's allegations (and reasonable inferences therefrom) to argue that Defendants lack significant contacts with the United States. ECF 73 at 25. In light of this, the Court should exercise its "broad discretion" to permit jurisdictional discovery. *Data Disc, Inc. v. Sys. Tech. Assocs., Inc.*, 557 F.2d 1280, 1285 n. 1 (9th Cir. 2007).

Jurisdictional discovery is appropriate "where pertinent facts bearing on the question of jurisdiction are controverted or where a more satisfactory showing of the facts is necessary." *Id.* A court should not deny discovery when the denial "will result in actual and substantial prejudice to the complaining litigant (*e.g.*, a reasonable probability that the outcome would have been different had discovery been allowed)." *Ali v. Carnegie Inst. of Wash.*, 967 F.Supp.2d 1367, 1372 (D. Or. 2013) (cleaned up).

Limited discovery is appropriate here in light of Defendants' unsupported assertion that Alhathloul alleges "no…actions" to exfiltrate her data and that Defendants only accessed Alhathloul's device *once*, "when it was located *outside* the forum." ECF 73 at 12-13 (emphasis in original). Contrary to that assertion, the Amended Complaint details how Defendants exerted significant control over the malware used to exfiltrate her data, including the ability to "command the malware to collect and transfer specific data, run additional exploits, or uninstall itself to avoid future detection." ECF 54 ¶ 126. Jurisdictional discovery regarding the technical specifications of the malware Defendants used to exfiltrate her data, and the manner in which Defendants controlled this malware to gain ongoing access to the data on Alhathloul's device, is necessary to rebut Defendants' characterization.

Defendants also contend that the Amended Complaint lacks sufficient detail to support Alhathloul's reasonable inference that the location of Defendants' "anonymization services and proxy servers…mattered to Defendants." ECF 73 at 15. Although the Amended Complaint already details how these "enhancements…masked the true origin," ECF 54 ¶ 107, of Defendants' transmissions to Apple (a U.S.-based company)—and therefore that the location of these anonymization services and proxy servers mattered—jurisdictional discovery should be

granted to the extent the Court determines "a more satisfactory showing of the facts is necessary." *Data Disc*, 557 F.2d 1285, n. 1.

A. Alhathloul Should be Granted Discovery Regarding the Malware Defendants Used to Exfiltrate Her Data and the Manner in Which Defendants Used it to Exfiltrate Her Data.

Limited jurisdictional discovery is appropriate in light of Defendants' unsupported assertion that they did not *act* to exfiltrate data from her device while it was located in the United States. Defendants argue that they did not access her device in the forum because, in their mistaken view, Alhathloul only alleges that Defendants "accessed Plaintiff's phone when it was located *outside* the forum, *then* Plaintiff carried the phone" as it transmitted data. ECF 73 at 12 (emphasis in original). They misconstrue Alhathloul's allegations in support of their argument that once the malware was implanted on her device, they took no further actions to exfiltrate her data because "the phone" autonomously transmitted data. *Id.* at 12-13.

But the allegations in the Amended Complaint, and reasonable interferences therefrom, suggest otherwise. The Amended Complaint alleges that Defendants exerted continuous control over the malware implanted on, and through which they exfiltrated data from, her device. Specifically, Paragraph 126 of the Amended Complaint alleges that "[t]he malware exfiltrate[d] data from the iPhone to the server" and that Defendants exerted control over the malware by "command[ing] the malware to collect and transfer specific data, run additional exploits, or uninstall itself to avoid future detection." ECF 54 ¶ 126. These allegations support a reasonable inference that Defendants' hacking conduct occurred not only through their omission—*see* ECF 73 at 13 (arguing that Defendants only failed "to engage in additional conduct to cease the alleged flow of information from her device")—but also their *actions*, by sending commands to the malware and compelling the ongoing transfer of Alhathloul's data to Defendants' servers.

Whether Defendants executed these commands by physically pressing a button, or by configuring their system to "automatically" and "continuously" occur, has no bearing on Defendants' jurisdictionally relevant conduct to access Alhathloul's device in the forum.[1] In any event, Defendants' assertion that they took no further action to exfiltrate Alhathloul's data once it was infected with malware improperly excludes both possibilities.

The manner in which exfiltration occurred, and the level of control Defendants exerted over the malware, are discoverable facts that bear directly on this Court's jurisdictional inquiry. As set out in Alhathloul's Opposition, case law shows that express aiming is satisfied when a defendant accesses a plaintiff's protected computer in the forum to commit a tort.[2] ECF 70 at 28 (collecting cases). Defendants' central argument for why this precedent is "inapposite" hinges on their unsupported assertion that "Plaintiff alleges no such 'actions'" to exfiltrate data from her device because, once infected with malware, "the phone" autonomously "transmit[ted] data." ECF 73 at 12-13 (brackets in original).

Discoverable facts regarding the malware Defendants used to exfiltrate Alhathloul's data, including the degree to which Defendants controlled or commanded the malware, would strengthen Alhathloul's showing that this Court has personal jurisdiction. Accordingly, there is no merit to Defendants' suggestion that Alhathloul's allegations suffer from an "endemic" flaw that should preclude jurisdictional discovery. *See* ECF 74 at 3. To the contrary, jurisdictional discovery regarding these matters should be granted based on the "reasonable probability" that

[1] In either case, each illegal exfiltration is a separate *intentional* act to access Alhathloul's device, and Defendants have not disputed that Alhathloul alleges an intentional act. *See* ECF 63 at 14 ("Although Plaintiff alleges an intentional act…").

[2] Alternatively, Defendants availed themselves of the forum by committing tortious conduct in the forum. ECF 70 at 24-25.

additional facts would strengthen Alhathloul's jurisdictional arguments. *Ali*, 967 F.Supp.2d 1372. Specifically, Alhathloul seeks discovery regarding: (1) the code that comprised the malware used to exfiltrate data from Alhathloul's device; (2) the system architecture of Karma showing the pathway of interactions between Alhathloul's device and Defendants' servers; (3) the commands sent by Defendants to the malware on Alhathloul's device; (4) Defendants' awareness of Alhathloul's physical presence in the United States.[3]

B. Alhathloul Should be Granted Jurisdictional Discovery Regarding the Identity, Nature, and Purpose of the Anonymization Services and Proxy Servers Utilized by Defendants.

Limited jurisdictional discovery is also appropriate to allow Alhathloul to show the jurisdictional significance of Defendants' use of U.S.-based anonymization services and proxy servers. Contrary to Defendants' assertion that "Plaintiff does not contend that the alleged location of the anonymization services and proxy servers in the United States (versus anywhere else) mattered to Defendants," ECF 73 at 15, the Amended Complaint details how these U.S.-based anonymization services and proxy servers "enhance[d] the effectiveness of" Karma by "prevent[ing] detection and mask[ing] the true origin" of Defendants' hacking transmissions. ECF 54 ¶¶ 105, 107-08. Taken together with Alhathloul's allegation that Defendants sought to "overcome evolving iOS security upgrades put in place by Apple" (a U.S.-based company), the Amended Complaint supports the inference that Defendants "cho[se] to use U.S.-based

[3] The Amended Complaint alleges two ways Defendants knew about Alhathloul's physical presence in the United States: the exfiltration of location data from her device and that her trip was widely publicized on social media. ECF 54 ¶¶ 142, 144-46. Nonetheless, Defendants argue that additional facts establishing their awareness of her presence in the United States are necessary. Alhathloul therefore seeks discovery to establish Defendants' knowledge of her location in the United States.

anonymization services and proxy servers" *because of* their U.S. connection. *See* ECF 54 ¶ 93; ECF 70 at 19.

However, to the extent a more satisfactory showing of the facts is necessary—which is what Defendants seem to contend—Alhathloul requests limited jurisdictional discovery to gather facts about the anonymization services and proxy servers that Defendants used. These facts can only be ascertained from Defendants. Specifically, Alhathloul seeks discovery regarding: (1) the identity of the companies Defendants procured anonymization services and proxy servers from; (2) the exact services Defendants procured, including the contract or agreement Defendants entered into; (3) the role and purpose of these services and proxy servers in furthering hacking activity, including how these anonymization services and proxy servers interacted with other technical features of Karma; (4) the reason for choosing these particular anonymization services and proxy servers.

CONCLUSION

For the foregoing reasons, and should the Court not be inclined to deny Defendants' Joint Motion to Dismiss based on the sufficiency of Alhathloul's allegations, the Court should grant Alhathloul's request for limited jurisdictional discovery. Further, the Court should hold in abeyance Defendants' Joint Motion to Dismiss pending the completion of jurisdictional discovery and order that the parties confer and submit a joint proposed discovery and briefing schedule on jurisdictional discovery within 14 days of the Court's order.

Dated: December 26, 2023 /s Christopher E. Hart

BOISE MATTHEWS DONEGAN LLP
Bridget M. Donegan
OSB No. 103753
805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

FOLEY HOAG LLP
Christopher E. Hart
MA BBO No. 625031
Anthony D. Mirenda
MA BBO No. 550587
Andrew Loewenstein
MA BBO No. 648074
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1000
chart@foleyhoag.com
adm@foleyhoag.com
aloewenstein@foleyhoag.com

ELECTRONIC FRONTIER FOUNDATION
David Greene
CA Bar No. 160107
Sophia Cope
CA Bar No. 233428
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
davidg@eff.org
sophia@eff.org

CENTER FOR JUSTICE AND ACCOUNTABILITY
Daniel McLaughlin
CA Bar No. 315326
Claret Vargas
MA BBO No. 679565
Carmen Cheung Ka Man
NY Bar No. 4132882
268 Bush St. #3432
San Francisco, CA 94104
(415) 544-0444
dmclaughlin@cja.org
cvargas@cja.org
ccheung@cja.org

Attorneys for Plaintiff Loujain Hathloul Alhathloul